

W



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,353	12/21/2000	Michael Nolte	6400-11WOUS	1134

7590 01/13/2005

McCormick Paulding & Huber
City Place II
185 Asylum Street
Hartford, CT 06103-4102

EXAMINER

POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/720,353	Applicant(s) NOLTE, MICHAEL	
	Examiner Peter Poltorak	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 7/2/2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2-11 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2-11 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on _____ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The amendment, and remarks therein, received on 7/02/2004 have been entered and carefully considered.
2. The amendment added a new independent claim 11 replacing claim 1.
3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

4. Applicant's arguments have been carefully considered but they were not found persuasive.
5. As per the argument that *Deo* does not teach a one-time encryptor (*pg. 9second §*) the examiner refers Applicant to HMAC as taught in col. 26, lines 7-23.
6. As per claim 1 (now pertaining to claim 11) Applicant argues that "the elements of claim 1 and the order in which they are presented are not present in the *Deo* reference." However, the applicant does not provide any specifics besides the arguments as discussed above (§ 5, above).
7. As per the argument that *Deo* does not disclose a control center having a first memory for a secret key the examiner refers Applicant to col. 26 lines 7-23 wherein *Deo* teaches a control center (*Content Provider*) producing a signing key by means of one-time encryption. Memory is inherently used in the process as disclosed by *Deo*.
8. Applicant argues that *Deo* does not disclose a receiver containing a corresponding memory that contains the same key. However, *Deo* discloses that a receiver using

Art Unit: 2134

the one-time encryption and the main key decrypts the message (*Deo*, col. 28 lines 1-24). Memory is inherently used to store keys during the decryption process.

9. As per the argument that *Deo* does not disclose or teach the generation of sequence number pairs by a generator in a control center in addition to the main key the examiner refers Applicant to fig. 9A and col. 26, lines 7-23, wherein *Deo* discloses the control center producing a sequence number (*message specific data*) and using the sequence number and the main key to produce a signing key.
10. As per the argument that *Deo* does not teach or remotely suggest the production of a signing key provided in advance with the main key to sender the examiner points out that "proving signing key in advance" is not found in claim 1 or new claim 11. Also, the claim language does not suggest providing sender with the main key. The main key is used to produce a signing key and the signing key is provided to the sender (*fig. 9A and col. 26, lines 7-23*).
11. As per the argument that *Deo* does not disclose using generated sequence numbers with the main key to generate a check key to verify the signature of the message in the receiver the examiner refers Applicant to col. 28, lines 1-4 wherein *Deo* discloses the receiver determining the sequence number, forming the one check key using the one-time encryption and the main key. If these steps were not present the receiver would not be able to decrypt the message as disclosed by *Deo* in col. 28 lines 1-24.
12. As per the newly introduced limitation in claim 11: "wherein the control center and the receiver share an undiscoverable main key" *Deo* teaches that control center first

Art Unit: 2134

obtains the current broadcast key which is currently stored on the receiver (*mobile device, col.26 lines 7-8*).

13. As a result, Applicant's suggestion that claims 2-7 are likewise deemed not anticipated or obvious by *Deo* for the reasons set forth for claim 1 is not persuasive.
14. As per claim 8 Applicant argues that the problem solved by applicant's invention, e.g. to specify a method for corruption protection of messages by means of a signature is not met. The examiner reminds Applicant that the purpose of the examination process is to determine whether the invention is patentable based on the claim language and not intended use of the invention. Replay attacks are well known threat in the art of communication security. As a result, maintaining a list of already used sequence numbers as taught by *Horstmann* (col. 5 lines 21-27) would have been obvious to one of ordinary skill in the art at the time of applicant's invention.

Priority

15. Foreign priority has been claimed in this application.

Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Germany on 4/30/1999. It is noted, however, that applicant has not filed a certified copy of the German application as required by 35 U.S.C. 119(b).

16. The effective priority date for the subject matter in the pending claims in this application once the paper has been received will be 4/30/1999.

Claim Rejections - 35 USC § 112

Art Unit: 2134

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

17. Claims 2-8 and 11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
 18. Claim 7 term: "in advance" (*produces a number of signing keys in advance*) is not understood.
 19. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
 20. The statement in claim 11: "providing a control center, a sender and a receiver..." is not understood. It is not clear whether something is missing or whether the limitation simply introduces the parties, which implement the method. Furthermore claim 11 is missing the step of signing a message.
 21. The "undiscoverable main key" (*claim 11*) is not understood. It is not clear to what the term: "undiscoverable" refers to.
 22. The "common main key" in claim 11 lacks antecedent basis. The examiner treats the "common main key" as the "undiscoverable main key".
 23. Claims 2-8 are rejected by being dependent on canceled claim 1.
- Appropriate correction is required.

Upon further search the following art was found: *Hoffmann et al. (U.S. Patent No. 5608800)* that reads on claims 9-10.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

24. Claims 9 and 11 are rejected under 35 U.S.C. 102(b) as being anticipated by *Hoffmann et al. (U.S. Patent No. 5608800)* and claims 2-7 would be rejected under the same paragraph once their dependencies are corrected.
25. As per claim 11 *Hoffmann et al.* teach a control center producing one or more sequence numbers (*random data Z*), and using one of the sequence numbers and the common main key (*coupling data K*) creating a signing key (*symmetric key E*) by means of one-time encryption (*col. 3 lines 37-43*). The signing key and the sequence number is provided to the sender via a secure transmission. (a control center and a sender are both within a transmitter) and the sender using the signing key forms a signature for a message (*col. 1 lines 44-46 and col. 3 lines 19-22*). Furthermore *Hoffman et al.* teach a control center sharing undiscoverable main key with a receiver as well as sending the message to the receiver via a data set containing at least the message and the (*enciphered*) signature (*S/E*) (*col.3 lines 45-52*). *Hoffman et al.* teach determining the sequence number from the received data set (*col. 3 lines 65-67*), passing the sequence number through a one-time encryption

Art Unit: 2134

to produce a check key (*col. 4 lines 1-3*) and using the check key to verify the signature of the message (*col. 4 lines 4-7*).

26. *Hoffman et al.* teach the limitation of claim 5 in col. 3 lines 37-38.

27. Claims 2-7 are substantially equivalent to the limitations of claim 11; therefore claims 2-7 are similarly rejected.

28. As per claim 9 the control center and the receiver inherently use memory. Any data operation includes memory, and inputs as well as outputs of data or mechanisms operating on data are connected to memory. Furthermore *Hoffman et al.* teach generator generating a sequence number (*col. 3 lines 35-36*) and the sequence number is used to generate a signing key (*symmetric key*) using one-way enciphering, which reads on one input of a first one-time encrypter being connected to a generator for a sequence number. One-time encrypter generates the signing key that is used to create a signature which is sent from the sender to the receiver (*refer to arguments per claim 11*), which reads on an output of the one-time encrypter being connected to the sender via a transport medium. Signature generator is inherently connected to the output of the one-time encrypter (*output, that is the signing key*) and to the message to be signed. *Hoffman et al.* teach data message block (*message*) being sent from the sender to the receiver (*col. 3 lines 49-52*), which reads on an output of the signature generator being connected to a device which assembles at least the signature and the message to form a data message block and whose output is connected to the receiver via a transport medium. Fig. 4 shows a signature checker having input connected to the message

Art Unit: 2134

and to the signature and an output of a second one-time encrypter and the input of the second one-time encrypter being connected to a means for providing a sequence number.

Claim Rejections - 35 USC § 103

29. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

30. Claim 8 is newly rejected under 35 U.S.C. 103(a) as being unpatentable over

Hoffmann et al. (U.S. Patent No. 5608800) in view of *Horstmann (U.S. Patent No 6009401)*.

31. As per claim 8 *Hoffmann et al.* teach the receiver as discussed above. *Hoffmann et al.* does not explicitly teach the receiver maintaining a list of already used sequence numbers, and rejects already used sequence numbers. *Horstmann et al.* teach a receiver (*the clearinghouse*) maintaining a list of already used sequence numbers (*used tickets*) and rejects already used sequence numbers (*Horstmann et al., col. 5 lines 21-27*). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to maintain a list of already used sequence numbers by a receiver and reject already used sequence numbers as taught by *Horstmann et al.*. One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid a replay attacks (*Horstmann et al., col. 5 line 22-23*).

Art Unit: 2134

32. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Hoffmann et al.* (U.S. Patent No. 5608800) in view of *Official Notice*.

33. *Hoffmann et al.* teach random number generator as discussed above. *Hoffmann et al.* do not teach the generator producing a sequence number using a deterministic method. *Official Notice* is taken that it is old and well-known practice to use deterministic methods to produce numbers. One of ordinary skill in art at the time of applicant's invention would employ deterministic method number generation in order to have control over number generation wherein given the same input the same output could be generated.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Signature

1/3/5

Date



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100